

ACADEMIC
PRESS

Journal of Algebra 255 (2002) 135–147

JOURNAL OF
Algebrawww.academicpress.com

Index of nilpotency of binomial ideals

Ignacio Ojeda Martínez de Castilla^{a,*,1} and
Ramón Piedra Sánchez^{b,1}^a *Departamento de Matemáticas, Universidad de Extremadura, Avda. de Elvas s/n,
E-06071 Badajoz, Spain*^b *Departamento de Álgebra, Universidad de Sevilla, Apdo. 41160, E-41080 Sevilla, Spain*

Received 31 May 2001

Communicated by Craig Huneke

Abstract

In this paper, we study and compute bounds for the index of nilpotency of lattice and cellular binomial ideals which are optimal in many cases. This computations can be generalized to binomial ideals, getting an effective Hilbert's Nullstellensatz for binomial ideals.

© 2002 Elsevier Science (USA). All rights reserved.

Keywords: Index of nilpotency; Binomial ideals; Lattice ideals; Semigroup ideals; Cellular decomposition; Effective Nullstellensatz

1. Introduction

Let $S := k[x_1, \dots, x_n]$ be the polynomial ring in n variables over a field k . Throughout this paper \mathbf{x}^α will denote the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_0^n$.

Given an ideal I in S there exists an integer e such that

$$(\sqrt{I})^e \subseteq I.$$

* Corresponding author.

E-mail addresses: ojedamc@unex.es (I. Ojeda), piedra@algebra.us.es (R. Piedra).

¹ Both authors are partially supported by Universidad de Sevilla, and by MCyT BFM2000-1523.

The *index* or *degree of nilpotency* $\text{nil}(I)$ of I is the smallest such integer e . In some texts the index of nilpotency is also called the *exponent* of I .

The existence of the index of nilpotency is always assured, but the computation of this integer or a bound of it are not easy at all.

The classical bounds are due to W.D. Brownawell [2], L. Caniglia, A. Galligo, and J. Heintz [3], and J. Kollár [10] as a consequence of effective Hilbert's Nullstellensatz. They only depend on the degree and number of generators of I . So, they are not uniquely defined: obviously, bounds obtained from irredundant systems of generators are usually smaller than the bounds getting from Gröbner bases.

We restrict our study to the class of *binomial ideals* in the polynomial ring S and present an effective method to compute bounds of the index of nilpotency which, in some cases, are much smaller than the known ones.

A *binomial* in S is an element with at most two terms, say $ax^\alpha - bx^\beta$, where $a, b \in k$ and $\alpha, \beta \in \mathbb{Z}_0^n$. A binomial ideal is an ideal in S generated by binomials. More precisely one have the following statement.

Proposition 1.1. *Let I be a binomial ideal in S . The reduced Gröbner basis of I with respect to any monomial order consists of binomials.*

It is known (cf. [5]) that every binomial ideal can be written as intersection of *cellular binomial ideals* (Definition 2.3). Thus, given a binomial ideal I in S it suffices to compute bounds for the index of nilpotency of its cellular components in order to get a bound for the index of I (Proposition 3.1). Cellular binomial ideals are easier to study, in part because they are strongly related with *lattice ideals* (Definition 2.2). So, we compute bounds for the index of nilpotency of cellular binomial ideals in terms of the index of nilpotency of the lattice ideals associated with (Theorem 3.1), in particular, these bounds are optimal when such lattice ideals are radical (Corollary 3.1). Thus, it is enough to compute bounds for the index of nilpotency of lattice ideals in order to bound the index of nilpotency of binomial ideals in general.

Lattice ideals are studied in greater depth in many papers; they are just a generalization of toric ideals [6,15] or semigroup (commutative, cancellative, and finitely generated) ideals [8,16].

Before to present our main result it is necessary to recall the concept semigroup ideals.

Let \mathcal{A} be a finitely generated commutative cancellative semigroup with zero element. Let $\{a_1, \dots, a_n\}$ be a fixed set of generators for \mathcal{A} . Consider the semigroup morphism

$$\pi : \mathbb{N}^n \rightarrow \mathcal{A}, \quad \mathbf{u} = (u_1, \dots, u_n) \mapsto u_1 a_1 + \dots + u_n a_n.$$

The map π lifts to an epimorphism of semigroup algebras:

$$\hat{\pi} : S = k[\mathbb{N}^n] \rightarrow k[\mathcal{A}] = \bigoplus_{m \in \mathcal{A}} k\{m\}, \quad x_i \mapsto 1 \cdot \{a_i\},$$

where $\{m\}$ denotes the symbol of $m \in \mathcal{A}$ in $k[\mathcal{A}]$.

The kernel of $\hat{\pi}$ is denoted by $I_{\mathcal{A}}$ and called *semigroup ideal* of \mathcal{A} . Besides, when \mathcal{A} is torsion free, $I_{\mathcal{A}}$ is also called *toric ideal*. The next lemma specifies an infinite generating set for the semigroup ideal $I_{\mathcal{A}}$.

Lemma 1.1. *The semigroup ideal $I_{\mathcal{A}}$ is spanned as a k -vector space by the set of binomials*

$$\{x^u - x^v \mid u, v \in \mathbb{N}^n, \pi(u) = \pi(v)\}.$$

In relation to the ideal $I_{\mathcal{A}}$, our main result, in particular, states:

Theorem 1.1. *Let \mathcal{A} be a finitely generated, commutative and cancellative semigroup, and \mathcal{G} the smallest group containing \mathcal{A} . If $p = \text{char}(k)$ and $m_1 p^{h_1}, \dots, m_r p^{h_r}$ are the invariant factors of \mathcal{G} , with $\prod m_i$ being not a multiple of p , then*

$$\text{nil}(I_{\mathcal{A}}) \leq \sum_{i=1}^r p^{h_i} - r + 1.$$

Furthermore, if k is algebraically closed then equality holds.

All this summarizes the results in the third section where we include also some examples in which our bounding methods are used. We would like to point out Remark 3.2 where we give an answer to Question 9.2.1 in [17].

Finally, since we can get bounds for the index of nilpotency of binomial ideals, using a well-known result (Theorem 3.4) we derive an effective Hilbert Nullstellensatz from our bounds.

2. Notations, notions and general assumptions

We will recall some definitions and results in [5,12]. First of all, we consider the ring $k[x^{\pm}] := k[\mathbb{Z}^n] = k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ of Laurent polynomials with coefficients in k .

A *binomial* in $k[x^{\pm}]$ is an element with at most two terms, say $ax^{\alpha} - bx^{\beta}$, where $a, b \in k$ and $\alpha, \beta \in \mathbb{Z}^n$. A *Laurent binomial ideal* is an ideal in $k[x^{\pm}]$ generated by binomials.

There exists a one-to-one correspondence between Laurent binomial ideals and partial characters.

Definition 2.1. A *partial character* on \mathbb{Z}^n is a homomorphism ρ from a sublattice \mathcal{L}_ρ of \mathbb{Z}^n to the multiplicative group $k \setminus \{0\}$.

Given a partial character (ρ, \mathcal{L}_ρ) , we associate a Laurent binomial ideal

$$I(\rho) = (\{x^\alpha - \rho(\alpha) \mid \alpha \in \mathcal{L}_\rho\}).$$

Note that in $k[x^\pm]$ every monomial is a unit, then any proper binomial ideal can be generated by elements in the form $x^\alpha - c_\alpha$ for some $\alpha \in \mathbb{Z}^n$ and $c_\alpha \in k \setminus \{0\}$. Theorem 2.1(a) in [5] states that every Laurent binomial ideal is associated to a unique partial character.

Laurent binomial ideals are strongly related to certain binomial ideals in S .

Definition 2.2. Given a partial character (ρ, \mathcal{L}_ρ) , we associate the following ideal in S

$$I_+(\rho) = (\{x^{\alpha_+} - \rho(\alpha)x^{\alpha_-} \mid \alpha \in \mathcal{L}_\rho\})$$

called *lattice ideal*, where α_+ and α_- denote the positive and negative part of α , respectively.

Proposition 2.1. A proper binomial ideal I in S is a lattice ideal if and only if $Ik[x^\pm] \cap S = I$.

Proof. [5, Corollary 2.5]. \square

This result can be also interpreted in the following way: a proper binomial ideal I is a lattice ideal if and only if every variable x_i is a nonzero divisor modulo I .

Remark 2.1. As a consequence of Lemma 1.1, every semigroup ideal is a lattice ideal with $\rho \cong 1$ and $\mathcal{L}_\rho = \{\alpha \in \mathbb{Z}^n \mid \pi(\alpha_+) = \pi(\alpha_-)\}$.

The following class of binomial ideals generalizes the concept of lattice ideal and primary ideal.

Definition 2.3. A proper ideal I in S is said to be *cellular* if, for some $\delta \subseteq \{1, \dots, n\}$, we have that

1. $Ik[\{x_i^\pm\}_{i \in \delta}][\{x_i\}_{i \notin \delta}] \cap S = I$.
2. For each $i \notin \delta$ there exists an integer $d_i \in \mathbb{Z}_+$ such that the ideal $(\{x_i^{d_i}\}_{i \notin \delta})$ contained in I .

In other words, an proper ideal I is cellular if every variable is either a nonzero divisor modulo I or is nilpotent modulo I .

Given any proper binomial ideal $I \subset S$, we can manufacture cellular binomial ideals from I as follows. For each vector of nonnegative integers $d = (d_1, \dots, d_n)$ and each subset δ of $\{1, \dots, n\}$, we set

$$I_\delta^{(d)} := (I + (\{x_i^{d_i}\}_{i \notin \delta}))k[\{x_i^\pm\}_{i \in \delta}][\{x_i\}_{i \notin \delta}] \cap S.$$

From Definition 2.3 it can be deduced that a proper binomial ideal I is cellular if and only if $I = I_\delta^{(d)}$ for some $\delta \subseteq \{1, \dots, n\}$ and $d \in \mathbb{Z}_0^n$.

Next result states the connection between lattice and cellular binomial ideals, but first we need one more piece of notation; we will write \mathbb{Z}^δ for $\{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n \mid \alpha_i = 0 \text{ if } i \notin \delta\}$, with $\delta \subseteq \{1, \dots, n\}$.

Proposition 2.2. *Let $I = I_\delta^{(d)}$ be a cellular binomial ideal in S . There exists a partial character (ρ, \mathcal{L}_ρ) on \mathbb{Z}^δ such that*

- (a) $I \cap k[\{x_i\}_{i \in \delta}] = I_+(\rho)$.
- (b) $\sqrt{I} = \sqrt{I_+(\rho)} + (\{x_i\}_{i \notin \delta})$.

Proof. [12, Proposition 2.2]. \square

3. Index of nilpotency of binomial ideals

Let $I = J_1 \cap \dots \cap J_r$ be some decomposition, not necessarily primary or irredundant. The homomorphism of rings

$$0 \rightarrow S/I \rightarrow \prod_{i=1}^r S/J_i$$

shows that

$$\sqrt{I}/I \hookrightarrow \prod_{i=1}^r \sqrt{J_i}/J_i$$

and therefore that

$$\text{nil}(I) \leq \max\{\text{nil}(J_i) \mid i = 1, \dots, r\}.$$

In [5], it is shown that every binomial ideal can be written as intersection of cellular binomial ideals, and, in [12], it is given an effective algorithm to compute this “cellular decomposition.” Then we have the following proposition.

Proposition 3.1. *Let I be a binomial ideal in S . If $I = J_1 \cap \dots \cap J_r$ is a cellular decomposition of I , then*

$$\text{nil}(I) \leq \max\{\text{nil}(J_i) \mid i = 1, \dots, r\}.$$

3.1. Index of nilpotency of cellular binomial ideals

Theorem 3.1. *Let $I = I_\delta^{(d)}$ be a cellular binomial ideal in S and $I_+(\rho) = I \cap k[\{x_i\}_{i \in \delta}]$, then*

$$\max_{m \in \mathcal{U}} \{\deg(m)\} < \text{nil}(I) \leq \text{nil}(I_+(\rho)) + \max_{m \in \mathcal{U}} \{\deg(m)\}$$

where \mathcal{U} is the set of monomials in $k[\{x_i\}_{i \notin \delta}] \setminus I$.

Proof. Since I is cellular with respect to $d \in \mathbb{Z}_0^n$ and $\delta \subseteq \{1, \dots, n\}$, then we have $(\{x_i^{d_i}\}_{i \notin \delta}) \subseteq I$. So we can assure that there are finitely many monomials in \mathcal{U} , thus the integer $e := \max_{m \in \mathcal{U}} \{\deg(m)\}$ is well defined. Now it straightforward follows that $(\{x_i\}_{i \notin \delta})^e \not\subseteq I$ and $(\{x_i\}_{i \notin \delta})^{e+1} \subseteq I$, and, by Proposition 2.2, $\sqrt{I} = \sqrt{I_+(\rho)} + (\{x_i\}_{i \notin \delta})$. Thus it is not hard to see that the statements $(\{x_i\}_{i \notin \delta})^{e+1} \subseteq I$ and $\text{nil}(I_+(\rho)) \geq 1$ implies $\text{nil}(I) \leq \text{nil}(I_+(\rho)) + e$, and that $(\{x_i\}_{i \notin \delta})^e \not\subseteq I$ gives the lower bound $e < \text{nil}(I)$. \square

Moreover, taking into account that $(\{x_i^{d_i}\}_{i \notin \delta})$ is contained in I , it immediately follows that $\max_{m \in \mathcal{U}} \{\deg(m)\} \leq \sum_{i \notin \delta} (d_i - 1)$. Therefore, the right hand inequality in Theorem 3.1 is also true replacing $\max_{m \in \mathcal{U}} \{\deg(m)\}$ by $\sum_{i \notin \delta} (d_i - 1)$; getting, by this way, “a priori” upper bounds for the index of nilpotency of cellular binomial ideals. In particular one has the equality if and only if the bigger monomial ideal in I is $(\{x_i^{d_i}\}_{i \notin \delta})$.

It can be checked that $\max_{m \in \mathcal{U}} \{\deg(m)\}$ is an upper bound for the numbers of terms in the Hilbert series of the zero dimensional ideal $I \cap k[\{x_i\}_{i \notin \delta}]$ with respect to the total degree monomial order. More precisely if M is the biggest monomial ideal contained in I , then $\max_{m \in \mathcal{U}} \{\deg(m)\}$ is the numbers of terms in the Hilbert series of M with respect to the total degree monomial order.

Note that if $I \cap k[\{x_i\}_{i \in \delta}]$ is radical then we have an equality in the left hand side of the formula in Theorem 3.1, in particular this happens when $\text{char}(k) = 0$ (cf. [5]). Thus we obtain a formula for $\text{nil}(I)$ in these cases.

Corollary 3.1. *Let $I = I_\delta^{(d)}$ be a cellular binomial ideal in S . If $I_+(\rho) = I \cap k[\{x_i\}_{i \in \delta}]$ is radical, then*

$$\text{nil}(I) = \max_{m \in \mathcal{U}} \{\deg(m)\} + 1,$$

where \mathcal{U} is the set of monomials in $k[\{x_i\}_{i \notin \delta}] \setminus I$. In particular, if $\text{char}(k) = 0$, then the equality above is true for every cellular binomial ideal in S .

Proof. It is enough to apply Theorem 3.1 with $\text{nil}(I_+(\rho)) = 1$. Finally, if $\text{char}(k) = 0$ then $I_+(\rho)$ is actually radical, even when k is not algebraically closed. \square

The next classical example, due to T. Mora, D. Lazard, D.W. Masser, P. Philippon, and J. Kollár (see [2]), provides a lower bound for the index of nilpotency of cellular binomial ideals.

Example 3.1. Let

$$I = (x_1^{d_1}, x_1 x_0^{d_2-1} - x_2^{d_2}, \dots, x_{n-2} x_0^{d_{n-1}-1} - x_{n-1}^{d_{n-1}}, x_{n-1} x_0^{d_n-1} - x_n^{d_n})$$

be an ideal in $k[x_0, x_1, \dots, x_n]$. Note that, I is a homogeneous binomial ideal and the given generators form a regular sequence.

The ideal I has a single associated prime $P = \sqrt{I} = (x_1, \dots, x_n)$, and it is easy to see that I is a cellular binomial ideal with respect to $\delta = \{0\}$ and $d = (*, d_1, d_1 d_2, \dots, \prod_{i=1}^n d_i)$, and $I \cap k[\delta] = (0)$. So, in this case, we can use Corollary 3.1 to compute exactly the index of nilpotency of I . Indeed, specializing in $x_0 = 1$, we have that

$$k[x_0, \dots, x_n]/(I, x_0 - 1) \cong k[x_n]/(x_n)^{\prod d_i}$$

and therefore we see that x_n is in the radical of I , but $(x_n)^{\prod d_i - 1}$ is not contained in I . Thus $\text{nil}(I) = \prod_{i=1}^n d_i$.

3.2. Index of nilpotency of lattice ideals

Definition 3.1. If \mathcal{L} is a sublattice of \mathbb{Z}^n , then the *saturation* of \mathcal{L} is the lattice

$$\text{Sat}(\mathcal{L}) := \{\alpha \in \mathbb{Z}^n \mid d\alpha \in \mathcal{L} \text{ for some } d \in \mathbb{Z} \setminus \{0\}\}.$$

Definition 3.2. If p is a prime number, we define $\text{Sat}_p(\mathcal{L})$ to be the largest sublattice of $\text{Sat}(\mathcal{L})$ containing \mathcal{L} such that $\mathcal{G} := \text{Sat}_p(\mathcal{L})/\mathcal{L}$ has order a power of p . If $p = 0$, we adopt the convention that $\text{Sat}_p(\mathcal{L}) = \mathcal{L}$.

Note that $\mathcal{G} \cong \mathbb{Z}/\mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}/\mathbb{Z}_{q_r}$, where each q_i is a power of p and $r \leq n$; they only depend on the group \mathcal{G} and are called the *invariant factors* of \mathcal{G} .

The invariant factors of a group can be computed in polynomial time in terms of elementary operations (cf. [9]).

Theorem 3.2. If $I = I(\rho)$ is a Laurent binomial ideal in $k[x^{\pm}]$, $\text{char}(k) = p$, and q_1, \dots, q_r are the invariant factors of $\text{Sat}_p(\mathcal{L}_\rho)/\mathcal{L}_\rho$, then

$$\text{nil}(I) \leq \sum_{i=1}^r q_i - r + 1.$$

Besides, if k is algebraically closed then equality holds.

Proof. If $p = 0$, then $\text{Sat}_p(\mathcal{L}_\rho)/\mathcal{L}_\rho = 0$. Therefore $\text{nil}(I) \leq 1$ which is trivially true because every Laurent binomial ideal is radical when $\text{char}(k) = 0$. So we may assume $p > 0$.

Now, suppose k algebraically closed. Since we have $\text{Sat}_p(\mathcal{L}_\rho)/\mathcal{L}_\rho \cong \mathbb{Z}/\mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}/\mathbb{Z}_{q_r}$, we can choose a basis $q_1\alpha_1, \dots, q_r\alpha_r$ for \mathcal{L}_ρ such that $\alpha_1, \dots, \alpha_r$ is a basis for $\text{Sat}_p(\mathcal{L}_\rho)$. Then, by Theorem 2.1(b) and Corollary 2.2 both in [5], $\mathbf{x}^{q_1\alpha_1} - \rho(q_1\alpha_1), \dots, \mathbf{x}^{q_r\alpha_r} - \rho(q_r\alpha_r)$, and $\mathbf{x}^{\alpha_1} - \rho'(\alpha_1), \dots, \mathbf{x}^{\alpha_r} - \rho'(\alpha_r)$, generate I and \sqrt{I} , respectively, where ρ' is the unique partial character of $\text{Sat}_p(\mathcal{L}_\rho)$ extending ρ . After a change of variables in $k[x^\pm]$ (cf. [5, Theorem 2.1(b)]) the ideals I and \sqrt{I} may be generated by $x_1^{q_1b_1} - c_1, \dots, x_r^{q_rb_r} - c_r$ and $x_1^{b_1} - c'_1, \dots, x_r^{b_r} - c'_r$, respectively, where $c'_i = \sqrt[q_i]{c_i}, i = 1, \dots, r$.

Setting $e := \sum_{i=1}^r (q_i - 1) + 1$, the former change of variables makes easy to check $(\sqrt{I})^e \subseteq I$ and, by elementary Gröbner basis arguments, it follows that $\prod_{i=1}^r (x_i^{b_i} - c'_i)^{q_i-1} \notin I$. So $(\sqrt{I})^{e-1} \not\subseteq I$ and $\text{nil}(I) = \sum_{i=1}^r (q_i - 1) + 1$.

In general, let \bar{k} be the algebraic closure of k . It is known that $I\bar{k} \cap k[x^\pm] = I$. Since $\text{nil}(I\bar{k}) = e$, one has

$$(\sqrt{I})^e = \left(\sqrt{I\bar{k}} \cap k[x^\pm] \right)^e \subseteq \left(\sqrt{I\bar{k}} \right)^e \cap k[x^\pm] \subseteq I\bar{k} \cap k[x^\pm] = I.$$

We conclude that $\text{nil}(I) \leq e = \sum_{i=1}^r (q_i - 1) + 1 = \sum_{i=1}^r q_i - r + 1$. \square

The equality in theorem above does not hold always as the next example shows.

Example 3.2. Let $k = \mathbb{Z}/\mathbb{Z}p(\alpha)$, where p is a prime number and $\sqrt[p]{\alpha} \notin k$. Consider the Laurent binomial ideal $I = (x^p - \alpha) \in k[x]$. Obviously $\text{nil}(I) = 1$, whereas $\text{nil}(I\bar{k}) = p$.

In spite of example above the hypothesis k algebraically closed is not actually necessary in order to have an equality in Theorem 3.2. It can be relaxed after suppose $c'_i \in k$ in the proof of Theorem 3.2, for every $i = 1, \dots, r$.

Although Theorem 3.2 it is true for any field k , it is quite difficult to use our arguments in order to give a close formula for the index of nilpotency in general (not only in the algebraically closed case). The main problem is that \sqrt{I} could not be binomial: consider $I = (x^p - \alpha, y^p - \alpha^2 - \alpha)$ in $\mathbb{Z}/\mathbb{Z}p(\alpha)[x, y]$, where p is a prime number and $\sqrt[p]{\alpha} \notin k$. These last questions is studied in greater depth in [1].

Finally, as an easy consequence of theorem above we have the following theorem.

Theorem 3.3. If $I = I_+(\rho)$ is a lattice ideal in S , $\text{char}(k) = p$ and q_1, \dots, q_r are the invariant factors of $\text{Sat}_p(\mathcal{L}_\rho)/\mathcal{L}_\rho$, then

$$\text{nil}(I) \leq \sum_{i=1}^r q_i - r + 1.$$

In addition, if k is algebraically closed then equality holds.

Proof. First of all, we will prove that $\sqrt{Ik[x^\pm]} = \sqrt{Ik[x^\pm]}$. The inclusion $\sqrt{Ik[x^\pm]} \supseteq \sqrt{Ik[x^\pm]}$ holds always. Conversely, let $f \in \sqrt{Ik[x^\pm]}$, then there exists a positive integer s such that $f^s \in Ik[x^\pm]$. On the other hand, one can find a monomial $m \in S$ which send f^s into $Ik[x^\pm] \cap S$, so, $m^s f^s \in Ik[x^\pm] \cap S$. But I is a lattice ideal, thus, by Proposition 2.1, $(mf)^s \in I$ and consequently $mf \in \sqrt{I}$. Finally, since monomials are units in $k[x^\pm]$, it follows $f \in \sqrt{Ik[x^\pm]}$.

If we set $e = \text{nil}(I)$, then $(\sqrt{I})^e \subseteq I$. By argument above it looks that

$$\left(\sqrt{Ik[x^\pm]}\right)^e \subseteq Ik[x^\pm].$$

Thus $\text{nil}(Ik[x^\pm]) \leq \text{nil}(I)$. On the other hand, if $e' = \text{nil}(Ik[x^\pm])$, then

$$(\sqrt{I})^{e'} = \left(\sqrt{Ik[x^\pm]} \cap S\right)^{e'} \subseteq \left(\sqrt{Ik[x^\pm]}\right)^{e'} \cap S \subseteq Ik[x^\pm] \cap S = I,$$

and so $\text{nil}(I) \leq \text{nil}(Ik[x^\pm])$. From both inequalities it follows that $\text{nil}(I) = \text{nil}(Ik[x^\pm])$ which implies the desired result. \square

Remark 3.1. Note that Theorem 1.1 is a consequence of the previous result (cf. Remark 2.1).

V. Ortiz established in [13] the existence of a canonical decomposition of ideals in a commutative noetherian ring. For him, the canonical P -primary component of an ideal I is the intersection of all P -primary components with minimal index of nilpotency. In the following example we will apply the index of nilpotency computation to get the canonical decomposition of binomial ideals.

The family of ideals used in the following example is taken from [4]. Primary decompositions of these ideals give useful descriptions of components of a graph arising in problems from combinatorics, statistics, and operations research.

Example 3.3. Let $I_{\mathcal{L}}$ be the prime ideal generated by all 2×2 -minors of

$$\begin{pmatrix} x_{11} & x_{12} & \dots & x_{1b} \\ x_{21} & x_{22} & \dots & x_{2b} \\ \vdots & \vdots & \ddots & \vdots \\ x_{a1} & x_{a2} & \dots & x_{ab} \end{pmatrix}$$

in $S = k[\{x_{ij}\}]$, where $a, b \geq 3$. Let $R := (x_{11}, x_{12}, \dots, x_{1b})$ and $C := (x_{11}, x_{21}, \dots, x_{a1})$. In [4], it is shown that the ideal of *corner minors* $I_{\mathcal{B}_{\text{cor}}} := (\{x_{11}x_{ij} - x_{1j}x_{i1} \mid 2 \leq i \leq a, 2 \leq j \leq b\})$ has the minimal primary decomposition

$$I_{\mathcal{B}_{\text{cor}}} = I_{\mathcal{L}} \cap R \cap C \cap (I_{\mathcal{B}_{\text{cor}}} + R^2 + C^2). \quad (1)$$

We will prove that

$$I_{\mathcal{B}_{\text{cor}}} = I_{\mathcal{L}} \cap R \cap C \cap \text{Hull}(I_{\mathcal{B}_{\text{cor}}} + (R + C)^3) \quad (2)$$

is the canonical decomposition, where $\text{Hull}(-)$ denotes the intersection of the minimal primary components of the corresponding ideal.

Note that the ideals $I_{\mathcal{L}}$, R , and C are prime, thus we can already assure that they are canonical components, it suffices to show that the fourth component is canonical too. In what follows we use the notation $Q := I_{\mathcal{B}_{\text{cor}}} + R^2 + C^2$. The radical of the primary ideal Q is $R + C$.

We first show that $\text{nil}(Q) \leq 3$. To see that, it suffices to check that $(R + C)^3 \subseteq R^2 + C^2 \subseteq Q$. Moreover, this implies that (2) is a minimal primary decomposition.

Note that $x_{12}x_{21} \in (R + C)^2$ does not lie in Q . So we can assure that $\text{nil}(Q) = 3$.

We next prove

$$I_{\mathcal{L}} \cap R \cap C \subseteq I_{\mathcal{B}_{\text{cor}}} + (R + C)^2. \quad (3)$$

Let $f \in I_{\mathcal{L}} \cap R \cap C$. Since $I_{\mathcal{L}}$ is a binomial ideal not containing any monomial, then by [5, Corollary 1.5], we can suppose f homogeneous of degree at least 2, that is, $f = m_1 - m_2$ with $\deg(m_1) = \deg(m_2) \geq 2$. On the other hand, since C is a monomial ideal and $f \in C$, the terms m_1, m_2 lie in C , thus we can write $m_1 = x_{i_1 1} m_{11}$ and $m_2 = x_{i_2 1} m_{12}$, with $\deg(m_{11}), \deg(m_{12}) \geq 1$; by the same argument on R , we have $m_1 = x_{1 j_1} m_{21}$ and $m_2 = x_{1 j_2} m_{22}$, with $\deg(m_{21}), \deg(m_{22}) \geq 1$. Therefore, either $m_1 = x_{11} m_{11} = x_{11} m_{21}$ or $m_1 = x_{i_1 1} x_{1 j_1} m_{31}$, with i_1 and j_1 not simultaneously equal to 1. If $m_1 = x_{11} m_{11}$, then

$$\begin{aligned} m_1 &= x_{11} m_{11} = x_{11} x_{kl} m_{41} \\ &= (x_{11} x_{kl} - x_{k1} x_{1l}) m_{41} + x_{k1} x_{1l} m_{41} \in I_{\mathcal{B}_{\text{cor}}} + (R + C)^2, \end{aligned}$$

otherwise $m_1 \in (R + C)^2$. In any case, $m_1 \in I_{\mathcal{B}_{\text{cor}}} + (R + C)^2$. Similarly, one can prove $m_2 \in I_{\mathcal{B}_{\text{cor}}} + (R + C)^2$. Therefore, $f = m_1 - m_2 \in I_{\mathcal{B}_{\text{cor}}} + (R + C)^2$, as desired.

By (3), we can assure that $I_{\mathcal{B}_{\text{cor}}}$ is strictly contained in $I_{\mathcal{L}} \cap R \cap C \cap (I_{\mathcal{B}_{\text{cor}}} + (R + C)^2)$. Thus, by [13, Theorem 2], it follows that (2) is the canonical decomposition of $I_{\mathcal{B}_{\text{cor}}}$, as claimed.

Using the improved version of Algorithm 9.6 in [5] given in [12], we have computed $\text{Hull}(I_{\mathcal{B}_{\text{cor}}} + (R + C)^3)$. In such a way we obtain that

$$I_{\mathcal{B}_{\text{cor}}} = I_{\mathcal{L}} \cap R \cap C \cap \left((I_{\mathcal{B}_{\text{cor}}} + (R + C)^3) : \left(\prod_{i, j \neq 1} x_{ij} \right)^{\infty} \right)$$

is the canonical decomposition which, in this case, is binomial. Although the canonical decomposition of a binomial ideal does not preserve binomiality, in general.

Remark 3.2. In [4] it is shown that $\text{in}_{\prec}(Q) = (R + C)^2$, where \prec denotes the reverse lexicographic term order and $x_{11} \prec x_{12} \prec \cdots \prec x_{1b} \prec x_{21} \prec \cdots \prec x_{ab}$.

Therefore, we have $3 = \text{nil}(Q) > \text{nil}(\text{in}_<(Q)) = 2$. This inequality provides a negative answer to Question 9.2.1 in [17] for this term order.

3.3. Application: an effective Nullstellensatz for binomial ideals

Hilbert's Nullstellensatz guarantees the existence of $g_1, \dots, g_t \in S$ such that $\sum f_i g_i = 1$, where f_1, \dots, f_t are polynomials in S with no common zero in \bar{k}^n . The usual proofs of this result, however, give no information about the g_i 's; for instance they give no bound on their degrees. It is here, one of the cases, where the index of nilpotency (or a bound of it) will play a crucial role, and vice versa.

Historically, it was G. Hermann [7] the first one who gave doubly exponential bounds for the degree of g_i 's in 1926. Later on, W.D. Brownawell [2], L. Caniglia, A. Galligo, and J. Heintz [3], and J. Kollár [10] obtained independently single exponential bounds. Nowadays, the effective Nullstellensatz keep on being an active research field as it can be seen through the abundant literature about it.

The following well-known theorem provides an effective Nullstellensatz in terms of the index of nilpotency.

Theorem 3.4. *Given f_1, \dots, f_t and $h \in S$, assume that h vanishes on all common zeroes of f_1, \dots, f_t (in the algebraic closure of k). If $I = (\bar{f}_1, \dots, \bar{f}_t) \subset S[x_0]$, then one can find $g_1, \dots, g_t \in S$ such that*

- (a) $\sum_{i=1}^t f_i g_i = h^{\text{nil}(I)}$;
- (b) $\deg(f_i g_i) \leq \text{nil}(I)(\deg(h) + 1)$, for each $i = 1, \dots, t$,

where \bar{f} denotes the homogenization of f with respect to the variable x_0 .

So, when $f_1 = \dots = f_t = 0$ is a binomial system of equations, the results in Section 3 provides bounds for $\text{nil}(f_1, \dots, f_t)$, which in many (binomial) cases improve the bounds known until now.

Example 3.4. Consider the polynomial system

$$\begin{aligned} f_1 &= 1 - x_1 x_2^d, & f_2 &= x_2 - x_3^d, & \dots, & & f_{n-1} &= x_{n-1} - x_n^d, \\ f_n &= x_n^2 \end{aligned}$$

in S , with $d \geq 2$. They have no common zero in the algebraic closure of k , then, by Bezout's version of the Nullstellensatz, there exist $g_1, \dots, g_n \in S$ such that $1 = \sum_{i=1}^n g_i f_i$. In [14], it is given, for this polynomial system, the following degree bound: $\deg(g_i f_i) \leq 2n^2 d$.

Using the results in the previous section and Theorem 3.4, we demonstrate that it is possible to find $g_1, \dots, g_n \in S$ such that

$$\deg(g_i f_i) \leq (n-1)(d-1) + 3, \quad i = 1, \dots, n.$$

To do that it is enough to prove $\text{nil}(I) = (n-1)(d-1) + 3$ with

$$I = (\overline{f_1}, \dots, \overline{f_n}) = (x_0^{d+1} - x_1 x_2^d, x_0^{d-1} x_2 - x_3^d, \dots, x_0^{d-1} x_{n-1} - x_n^d, x_n^2).$$

We only summarize the more relevant steps; for the complete proof and details see [11].

First, by Algorithm A.2 in [12], we have that

$$I = (I : x_1^\infty) \cap (I : x_2^\infty) \quad (4)$$

is an irredundant cellular decomposition, where $(I : x_1^\infty)$ and $(I : x_2^\infty)$ are cellular with respect to $\delta = \{1\}$ and $\delta = \{2\}$, respectively. Therefore, by Proposition 3.1, $\text{nil}(I) \leq \max\{\text{nil}(I : x_1^\infty), \text{nil}(I : x_2^\infty)\}$. Moreover, in this case, it is easy to check that equality holds. And now, using Corollary 3.1, we obtain $\text{nil}(I : x_2^\infty) \leq \text{nil}(I : x_1^\infty) = (n-1)(d-1) + 3$. Putting all this together, we have $\text{nil}(I) = (n-1)(d-1) + 3$, as desired.

In particular, when $n = d = 2$ one has $1 = (-1)f_1 + x_1 f_2$. In this case $\deg(g_1 f_1) = \deg(g_2 f_2) = 3 < \text{nil}(I) = 4$ which shows that our procedure provides a bound smaller than the other ones, although is not optimal.

References

- [1] E. Becker, R. Grobe, M. Niermann, Radical of binomial ideals, *J. Pure Appl. Algebra* 117&118 (1997) 41–79.
- [2] W.D. Brownawell, Bounds for the degrees in the Nullstellensatz, *Ann. of Math.* 126 (3) (1987) 577–591.
- [3] L. Caniglia, A. Galligo, J. Heintz, Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque, *C. R. Acad. Sci. Paris* 307 (1988) 255–258.
- [4] P. Diaconis, D. Eisenbud, B. Sturmfels, Lattice walks and primary decomposition, in: *Mathematical Essays in Honor of Gian-Carlo Rota*, Cambridge, MA, 1996, in: *Progr. Math.*, Vol. 161, Birkhäuser Boston, 1998, pp. 173–193.
- [5] D. Eisenbud, B. Sturmfels, Binomial Ideals, *Duke Math. J.* 84 (1) (1996) 1–45.
- [6] W. Fulton, Introduction to Toric Varieties, in: *Ann. of Math. Stud.*, Vol. 131, Princeton University Press, Princeton, 1993.
- [7] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.* 95 (1926) 736–788.
- [8] J. Herzog, Generators and relations of semigroups and semigroups rings, *Manuscripta Math.* 3 (1970) 175–193.
- [9] C.S. Iliopoulos, Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrix, *SIAM J. Comput.* 18 (4) (1989) 658–669.
- [10] J. Kollár, Sharp effective Nullstellensatz, *J. Amer. Math. Soc.* 1 (4) (1988) 963–975.
- [11] I. Ojeda, Ideales Binomiales y Aplicaciones, PhD thesis, Universidad de Sevilla, 2000, <http://cervantesvirtual.com/FichaObra.html?Ref=4451>.
- [12] I. Ojeda, R. Piedra, Cellular binomial ideals. Primary decomposition of binomial ideals, *J. Symb. Comput.* 30 (4) (2000) 383–400.
- [13] V. Ortiz, Sur une certaine décomposition canonique d'un idéal en intersection d'idéaux primaires dans un anneau noetherien commutatif, *C.R. Acad. Sci. Paris* 248 (24) (1959) 3385–3387.

- [14] M. Sombra, A sparse effective Nullstellensatz, *Adv. Appl. Math.* 22 (1999) 271–295.
- [15] B. Sturmfels, *Grobner Bases and Convex Polytopes*, in: *University Lecture Ser.*, Vol. 8, Amer. Math. Society, Providence, RI, 1995.
- [16] A. Vigneron, Semigroup ideals and linear diophantine equations, *Linear Algebra Appl.* 295 (1999) 133–144.
- [17] W. Vasconcelos, et al., *Computational Methods in Commutative Algebra and Algebraic Geometry*, in: *Algebra Comput. in Math.*, Vol. 2, Springer, New York, 1998.